anand guru

SOC EXPERTS

Interview Questions on
Web Application Security

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

Why should we focus on Web Application Security?

- Hacked Websites Target Your Customers - revoked licenses and legal proceedings.
- The number of hacked sites rises rapidly
- High value rewards, including sensitive private data collected from successful source code manipulation.
- Ease of execution, as most attacks can be easily automated and launched indiscriminately against thousands, or even tens or hundreds of thousands of targets at a time.
- Business reputation loss and drop in revenue
- Website clean-up is more expensive than protection
- Website gets blacklisted

The method of successfully phishing a user, installing malware, and remotely controlling the infected computer without anyone noticing did not have a very high success rate. In addition, finding the data to steal required time, and the longer an attacker remained in a network, it increased their chances of being caught.

As a result, attackers began to shift their focus to exploiting web application security vulnerabilities. These attacks are significantly more efficient and effective.

anand guru

What kind of attacks are web application vulnerable to?

According to OWASP (Open Web Application Security Project) the top 10 web application security vulnerabilities are :

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XEE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Using Components With Known Vulnerabilities
- Insufficient Logging And Monitoring

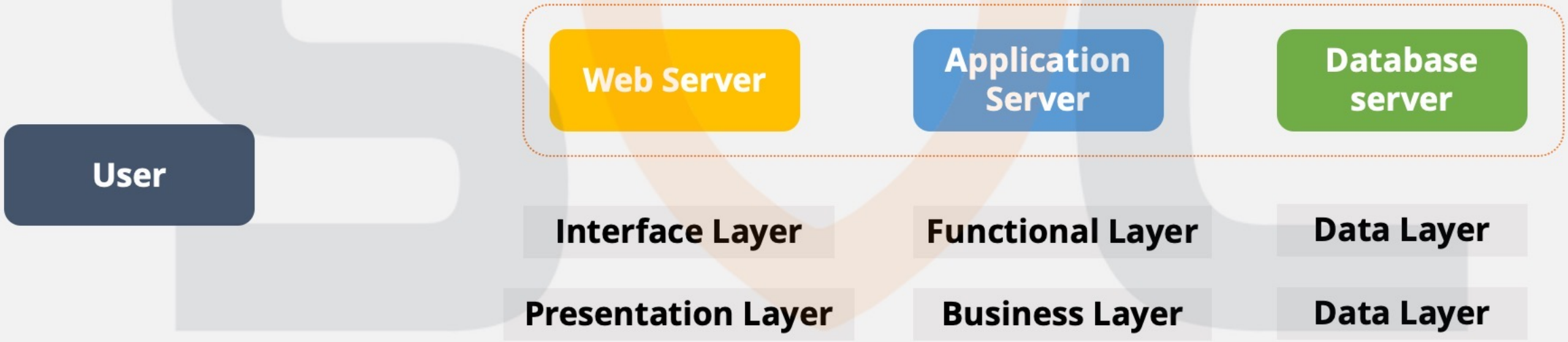
Other attacks that web application vulnerable to include,

- DOS/DDOS
- DNS Server Hijacking
- DNS Amplification Attack
- MITM/Sniffing Attack
- Website Defacement
- Web Cache poisoning attack

anand guru

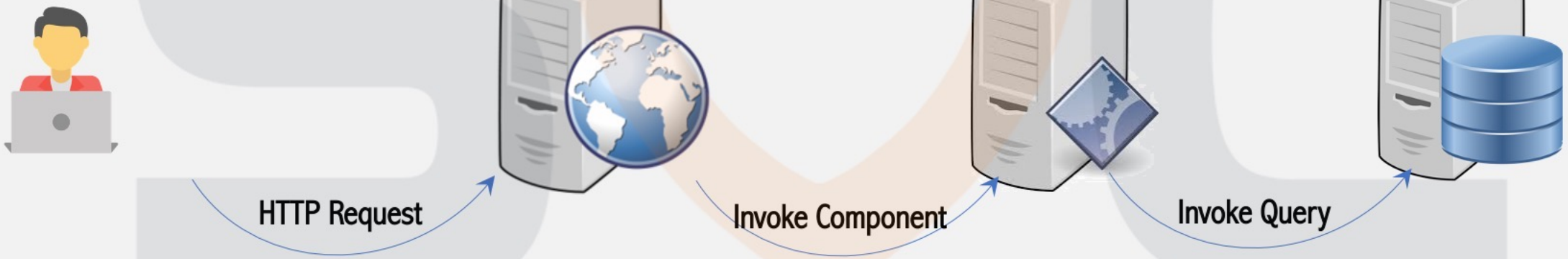
Explain a typical Web Application Server Architecture

Usually web application are deployed in 3-tier architecture.



anand guru

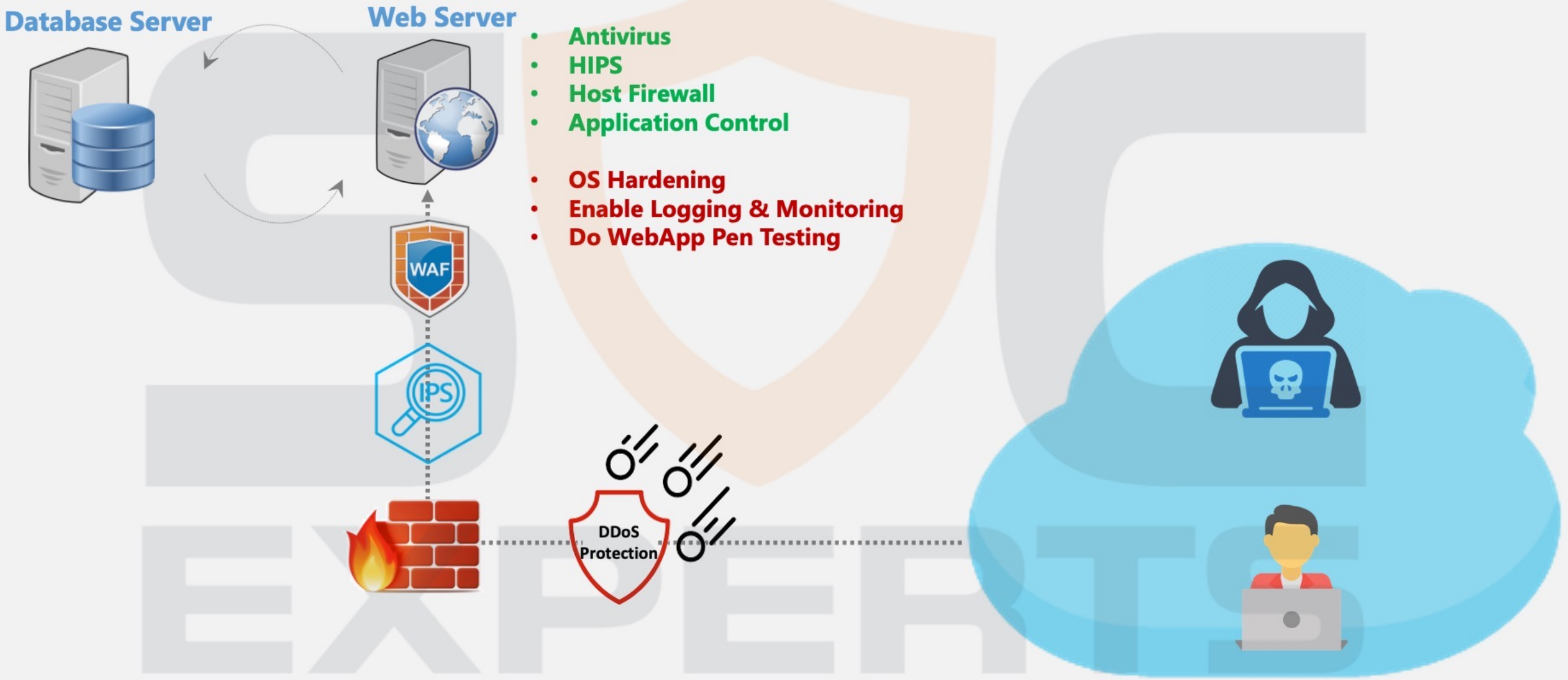
Explain a typical Web Application Server Architecture



anand guru

Explain layers of protection for a Web Application Server.

If budget is not a constraint how will you secure a web server?



- Antivirus
- HIPS
- Host Firewall
- Application Control

- OS Hardening
- Enable Logging & Monitoring
- Do WebApp Pen Testing

anand guru

What is System Hardening?

Systems hardening is a process of securing a system by reducing its attack surface.

Few things on the system hardening checklist include:

- Changing the default user credentials
- Closing all unused ports
- Stopping all unused services
- Install updates and patches
- Implement Access Control
- Install Antivirus and keep the signatures up-to-date

SOC EXPERTS

anand guru

Name the commonly used Web Servers.

anand guru

Explain HTTP protocol.

There are following three basic features which makes HTTP a simple but powerful protocol:

HTTP is connectionless: The HTTP client i.e. browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server process the request and re-establish the connection with the client to send response back.

HTTP is media independent: This means, any type of data can be sent by HTTP as long as both the client and server know how to handle the data content. This is required for client as well as server to specify the content type using appropriate MIME-type.

HTTP is stateless: As mentioned above, HTTP is a connectionless and this is a direct result that HTTP is a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different request across the web pages.

anand guru

Explain the HTTP request syntax.

```
GET /hello.htm HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE5.01; Windows NT)
Host: www.socexperts.com
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: Keep-Alive

userID=4321&userName=Anand+Guru
```

SOC EXPERTS

Explain different HTTP methods.

HTTP defines a set of request methods to indicate the desired action to be performed for a given resource.

Methods	Description
GET	The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.
HEAD	Same as GET, but transfers the status line and header section only.
POST	A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms.
PUT	Replaces all current representations of the target resource with the uploaded content.
DELETE	Removes all current representations of the target resource given by a URI.
CONNECT	Establishes a tunnel to the server identified by a given URI.
OPTIONS	Describes the communication options for the target resource.
TRACE	Performs a message loop-back test along the path to the target resource.

EXPERTS

anand guru

Explain HTTP Status Codes.

HTTP response status codes indicate whether a specific HTTP request has been successfully completed. Responses are grouped in five classes:

Classes	Description	Most Used	Description
Informational responses (100–199)	This interim response indicates that everything so far is OK and that the client should continue the request, or ignore the response if the request is already finished.	-	-
Successful responses (200–299)	This class of status code indicates that the client's request was successfully received, understood, and accepted.	200 OK 201 Created 204 No Content	The request has succeeded. The request has been fulfilled and resulted in a new resource being created. The server has fulfilled the request but does not need to return an entity-body
Redirects (300–399)	This class of status code indicates that further action needs to be taken by the user agent in order to fulfill the request.	301 Moved Permanently 304 Not Modified	The requested resource has been assigned a new permanent URI and any future references to this resource SHOULD use one of the returned URIs. Indicates the resource has not been modified since last requested.
Client errors (400–499)	The 4xx class of status code is intended for cases in which the client seems to have erred	400 Bad Request 401 Unauthorized 403 Forbidden 404 Not Found	The request could not be understood by the server due to malformed syntax. The request requires user authentication. The response MUST include a WWW-Authenticate header field The server understood the request, but is refusing to fulfill it. The server has not found anything matching the Request-URI.
Server errors (500–599)	Indicate cases in which the server is aware that it has erred or is incapable of performing the request.	500 Internal Server Error 503 Service Unavailable	The server encountered an unexpected condition which prevented it from fulfilling the request. The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.

anand guru

Few random questions.

What is Session?

A session can be defined as a server-side storage of information that is desired to persist throughout the user's interaction with the web site or web application. This is usually done by storing a session ID on the client side.

What is a Web Cookie?

A cookie is a small piece of text stored on a user's computer by their browser. Common uses for cookies are authentication, storing of site preferences, shopping cart items, and server session identification.

What is Robot.txt?

A robots.txt file tells search engine crawlers which pages or files the crawler can or can't request from your site.

What is Web Crawling?

Process of collecting information about a website. Crawling gives a blueprint of a website.

What is a Web Scraping?

Also referred to as web data extraction, is the process of downloading information from the website for later use.

anand guru

Questions on Apache logs.

What are the different logs of Apache server writes.

Apache has 2 types of logs:

Access Log

The access log contains information about requests coming in to the web server. This information can include what pages people are viewing, the success status of requests, and how long the server took to respond.

Error Log

The error log contains information about errors the web server encountered when processing requests, such as missing files. It also includes diagnostic information about the server itself.

What is the format of Apache web server logs?

Apache uses the **Common Log Format (CLF)** by default

What is the default log location for Apache web server?

Typically apache access logs are stored in **`/var/log/httpd/access_log`**

However on some flavor of Linux the logs are written to

`/var/log/apache2/access.log`

`var/log/httpd-access.log`

anand guru

Explain Apache Access log format.

Log Format: `%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\"`

Value	Std. Format	Description
127.0.0.1	%h	This is the IP address of the client (remote host) which made the request to the server
-	%l	The "hyphen" in the output indicates that the requested piece of information is not available. In this case, the information that is not available is the RFC 1413 identity of the client determined by identd on the clients machine.
frank	%u	This is the userid of the person requesting the document as determined by HTTP authentication.
[10/Oct/2000:13:55:36 -0700]	%t	The time that the server finished processing the request. The format is: [dd/mmm/yyyy:hh:mm:ss zone]
"GET /apache_pb.gif HTTP/1.0"	\"%r\"	The request line from the client is given in double quotes. The request line contains a great deal of useful information. First, the method used by the client is GET. Second, the client requested the resource /apache_pb.gif, and third, the client used the protocol HTTP/1.0
200	%>s	This is the status code that the server sends back to the client. This information is very valuable, because it reveals whether the request resulted in a successful response (codes beginning in 2), a redirection (codes beginning in 3), an error caused by the client (codes beginning in 4), or an error in the server (codes beginning in 5).
2326	%b	The last entry indicates the size of the object returned to the client, not including the response headers. If no content was returned to the client, this value will be "-".
"http://www.example.com/start.html"	\"%{Referer}i\"	This gives the site that the client reports having been referred from. (This should be the page that links to or includes /apache_pb.gif).
"Mozilla/4.08 [en] (Win98; I ;Nav)"	\"%{User-agent}i\"	The User-Agent HTTP request header. This is the identifying information that the client browser reports about itself.

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
"http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)"
```

What is the default log location for IIS web server?

IIS log files are stored by default in the **`%SystemDrive%\inetpub\logs\LogFiles`** folder of the IIS server.

Explain IIS Access log format.

IIS log file format

Syntax	`Client_IP Username Date Time Service&Instance Server_Name Server_IP Time_Taken Client_Bytes_Sent Server_Bytes_sent Status_Code Windows_Status_Code Request_Type Target_Operation Parameters`
Example	`192.168.114.201, -, 03/20/05, 7:55:20, W3SVC2, SERVER, 172.21.13.45, 4502, 163, 3223, 200, 0, GET, /DeptLogo.gif, -,`

W3C extended logging

Syntax	`date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)`
Example	`2002-05-02 17:42:15 172.22.255.255 - 172.30.255.255 80 GET /images/picture.jpg - 200 Mozilla/4.0+(compatible;MSIE+5.5;+Windows+2000+Server)`

anand guru

What is the default log location for IIS web server?

IIS log files are stored by default in the **`%SystemDrive%\inetpub\logs\LogFiles`** folder of the IIS server.

Explain IIS Access log format.

IIS log file format

Syntax	`Client_IP Username Date Time Service&Instance Server_Name Server_IP Time_Taken Client_Bytes_Sent Server_Bytes_sent Status_Code Windows_Status_Code Request_Type Target_Operation Parameters`
Example	`192.168.114.201, -, 03/20/05, 7:55:20, W3SVC2, SERVER, 172.21.13.45, 4502, 163, 3223, 200, 0, GET, /DeptLogo.gif, -,`

W3C extended logging

Syntax	`date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)`
Example	`2002-05-02 17:42:15 172.22.255.255 - 172.30.255.255 80 GET /images/picture.jpg - 200 Mozilla/4.0+(compatible;MSIE+5.5;+Windows+2000+Server)`

anand guru

What is WAF and how does it work?

- WAF is short for Web Application Firewall, and is a firewall for web applications.
- It is a way to protect network traffic at application level.

How does a Web Application Firewall work?

- A WAF examines and filters traffic to web applications.
- It keeps track of communication between the client and server and control access and decide what traffic should be blocked.
- A WAF protects against some of the most common cyber attacks, including SQL injections, cross-site scripting and (D)DoS attacks.
- Most WAFs are proactive and self-learning.
    - When you first define communication and access, you let the WAF monitor traffic for a period of time so that it can learn what legitimate traffic looks like. It then creates a default mode and the WAF can then keep track of unusual traffic patterns.

Name few popular WAF solutions.

Imperva	(Incapsula)
Cloudflare	(Web Application Firewall)
F5 Networks	(Advanced Web Application Firewall)
Fortinet	(FortiWeb)
Barracuda	(Web Application Firewall)

anand guru

What are the different types of protection a WAF provides?

- Like most of the device, WAF does a **IP reputation check**, blocking traffic from know bad actors in the internet.
- Next a WAF would **defend against** application level **DDOS attacks**
- Followed by that it does **protocol validation** to see if all requests match the HTTP RFC
- Then, it will look for **know application attacks** using **attack signatures.**
- A **antivirus module** will help WAF to block any malwares being uploaded to the server.
- Followed by this is **the advance protection engine** to detect **Scanners, Crawlers, Scrapers** etc.
- Finally, most of the modern day WAFs come with **machine learning based behavioral detection**.

EXPERTS

anand guru

Difference between WAF and Network Firewall.

Network Firewall	WAF
1. Works at Layer 3 and 4	1. Works at Layer 3 to 7
2. Does Packet filtering and Stateful inspection.	2. Signatures, App-specific Anomaly detection, Protocol Anomaly detection
3. Defend against intrusions by unauthorized users	3. Defend against Web Application attacks (XSS, SQLi, DDOS, Buffer Overflow etc.)
4. DDOS protection at network layer	4. DDOS Protection at Application Layer
5. Deployed at perimeter	5. Deployed behind perimeter firewall before the web server
6. Does not scan for SSL	6. WAFs scan SSL traffic
7. Do not perform load balancing	7. Performs load balancing of web traffic

anand guru

What tools are used for application penetration testing?

OWASP
Zed Attack Proxy

Nikto

anand guru

Have you dealt with any web attacks?

Scenario 1: Web defacement.

- Customer reported the issue to SOC.
- We immediately opened a bridge call and involved the SOC lead, network team and the application team.
- Client also called in the marketing and legal team.
- SOC team supplied the relevant data to other teams like:
  - Domain details
  - IP Address & Location
  - All the logs generated because of the IP address
  - OS, Webserver details
  - Defacer (Attacker) information
  - Snapshot of the Defaced page.
  - Source code of the Defaced page.
- It was decided to take down the website temporarily
- Vulnerability in WordPress libraries
- Led attackers to inject PHP objects (CVE-2018-20148)
- The vulnerability was immediately patched and the website was restored with a downtime of 4 hours

SOC EXPERTS

Have you dealt with any web attacks?

Scenario 2: DDoS Attack on FTP server

SIEM reported a possible DDOS attack. The logic of the correlation was to trigger when more than 500 IPs connect to one IP address with in 1 minute.

- *Analysis of the alert*
    - Access the service as a user to see if it is still up and running
    - Ran 'netstat –an' to check if there are several WAIT connections
    - Ran continuous pings to see if there are any packet drops
    - Check the bandwidth consumption on network monitoring tools (PRTG, Nagios)
    - Because the intensity was too high we opened the Bridge call
- *Remediation for the incident*
    - Opened a bridge call with the network team, ISP, application team, SOC lead/manager and Server team
    - Temporarily added more servers to load balance
    - Reduced the connection-wait-time at firewall level
    - Limited the No. of connection from an IP address
    - Blocked the top 5 or 10 IPs that are aggressively involved in the attack
    - Prepared to bring up the DR servers

anand guru